ANNUAL REPORT OF THE AUTOMATION AND TECHNOLOGY COMMITTEE TO THE ILLINOIS JUDICIAL CONFERENCE

Honorable Grant S. Wegner, Chairperson

Honorable Robert E. Byrne
Honorable James K. Donovan
Honorable Charles H. Frank
Honorable R. Peter Grometer
Honorable Robert J. Hillebrand
Honorable Thomas H. Sutton
Honorable Edna Turkington
Honorable David A. Youck

October 2002

I. STATEMENT ON COMMITTEE CONTINUATION

The Automation and Technology Committee ("Committee") of the Illinois Judicial Conference is charged with evaluating, monitoring, coordinating and making recommendations concerning automated systems for the Illinois judiciary. This is a formidable undertaking, given the variety of technological applications available to the courts. Technology affects, or has the potential to affect, nearly every operational and administrative judicial function. New and improved applications and devices are introduced regularly, each promising to bestow greater efficiency upon the judicial system and lower operating costs. Technology choices, moreover, must be made carefully, guided by thorough evaluation before resources are committed. The Committee occupies a unique position in this regard.

Since its inception the Committee has reviewed automation-related work being done by other judicial branch committees and justice agencies; surveyed Illinois judges' use of computers and other automated systems; evaluated a number of software applications; assisted in the development of a computer education program for judges; developed a web page concept for the Illinois judiciary, which was approved by the Judicial Conference and Supreme Court for implementation; distributed a computer security brief at the Education Conference 2002; and pursued a variety of other activities in fulfillment of its charge. Much remains to be accomplished. Accordingly, the Committee respectfully requests that it be continued.

II. SUMMARY OF COMMITTEE ACTIVITIES

During the 2002 Conference year, this Committee continued its efforts to provide computer security information to the Illinois judiciary. Toward that effort, the Committee developed and disseminated a computer security brief at the two sessions of the Education Conference 2002 which was held in February and March 2002. The brief was kept to a one page document containing eight bullets on computer security that was printed on stiff colored paper. The eight items were part of the draft model policy developed by the Committee during the 2001 Conference year. A stiff paper was selected to provide longevity and durability in hopes that the brief would be displayed at or near the judges' computer workstation. The brief also included a "plug" for the Supreme Court of Illinois' web page URL that debuted in April 2001 and contains numerous judicial links that can be of assistance to the Illinois judiciary. A copy of the brief is attached to this report as Appendix 1.

The Subcommittee on Computer Security continued to work on a model policy or list of components to be included in a policy on computer security guidelines and computer usage for judges. Their effort was expanded to include Internet access and email. Copies of existing circuit rules, policies, and on Internet access and email were requested from the chief circuit judges. The 16th, 18th, and 19th circuits provided a copy of their rules and policies for the subcommittee to review. A copy of the rules and policies are provided in Appendix 2.

The New Technologies Committee exchanged documents regarding new technologies between its members and the full committee. These documents covered such topics as: legal research, electronic filing, laptops and personal digital assistants (PDA) devices usage, a concept for a cyber jury café, wireless technology concepts, e-learning and e-book usages, data warehousing, etc. In addition to the new technologies reviewed, the subcommittee reviewed a book entitled, "Effective Use of Courtroom Technology, *A Judge's Guide to Pretrial and Trial*."

In particular, the subcommittee thought the book presented court technologies in a format that was easy to read and understand by a novice to technology. It explained in simple terms what considerations the court should give some of the new technologies parties are requesting to use in the courtrooms, such as electronic exhibits, video demonstrations, computer simulations, etc. It identified the need for the Court to assure equal use of technology by all parties. Some technologies are expensive and, therefore, not available to all parties, equally.

After review, consideration was given to a cost-effective method of providing it to all judges. That issue was quickly resolved when the subcommittee learned the book was available through the Administrative Office's (AOIC) Resource Lending Library. The subcommittee recommends the book to all judges and court administrators facing management issues on these technologies. The AOIC reference number for the book is 01-PB-064.

III. PROPOSED COMMITTEE ACTIVITIES FOR THE NEXT CONFERENCE YEAR

During the 2003 Conference year, the Committee will continue its work to develop model policy or list of components to be included in a policy on computer security guidelines and computer usage for judges, continue to evaluate existing and emerging technologies and legislation affecting court technology, work with the AOIC in the development of electronic filing and a statewide judicial information system or Intranet.

The members of the Committee look forward to the coming Conference year and appreciate the opportunity to be of service to the Supreme Court and the judicial branch.

IV. RECOMMENDATIONS

The Committee is making no recommendations to the Conference at this time.

2002 REPORT

APPENDIX 1

A COMPUTER SECURITY BRIEF

Computer security continues to be a top issue for today's judiciary, as well as other branches of government. The Automation and Technology Committee of the Illinois Judicial Conference offers the following brief guidelines for judges to consider.

- **Reason For Using The Computer:** The judge's computer should only be used for functions relating to performance within their judicial capacity.

- **Internet Policy (including e-mail):** An Internet Access Policy should be created within each county/circuit and the policy should be approved and signed by each judge.

- **Anti Virus:** Virus protection software should be installed and updated on a regular maintenance schedule. All computer files should be scanned weekly for viruses. Any files or information downloaded from the Internet or uploaded from CD's, discs or other media should be scanned prior to opening.

- **Passwords:** Password protection of information is a critical security measure. Passwords must be kept secret, should consist of at least six alphanumeric characters, and be changed every 30 days. Personal associations and words found in dictionaries should be avoided. Passwords should not be written down and posted near the work area.

- **Backup:** Backup files should be created for data files to protect against power failures, hardware failures, and diskette problems.

- **Copyright Infringement:** Awareness of the potential for copyright infringement is essential. Routine transmission of words, pictures, music, or computer software over computer networks can be a violation of the copyright infringement laws.

- **E-mail:** Before transmitting sensitive material, Email addresses should be verified. Email messages travel from server to server and sophisticated computer hackers can intercept, read, and alter messages. There is no right to privacy regarding e-mail. All correspondence should be considered to be "public."

- **Firewall:** There should be an awareness that accesses to the Internet may be limited by the use of a filter or firewall. The limits established by the firewall are generally determined by the governmental entity providing the computer equipment.

The Automation and Technology Committee highly recommends that all judges review the Supreme Court's Web Page. It is an excellent Internet site for the Illinois Judiciary, containing Supreme and Appellate Court Opinions, many options for automatically receiving information via Email, and extensive "links" to other judicial and legal research sites. The address is **WWW.STATE.IL.US/COURT**.

Recommendations and suggestions regarding computer security are welcome and may be submitted by mail to Dan Mueller, Staff Liaison, Computer Security Subcommittee, 840 S. Spring Street, Springfield, IL 62704 or by email at dmueller@court.state.il.us.

APPENDIX 2

16th Circuit, Kane County

INTERNET/INTRANET USAGE POLICY

WHEREAS, the Internet/intranet offers the County new methods of communication and new sources of information that can enhance the County's operating efficiency and effectiveness; and

WHEREAS, the County adopted Resolution 93-293 governing E-Mail usage and that resolution can be applied to Internet E-Mail usage; and

WHEREAS, the County adopted Resolution 97-184 governing Internet usage and that resolution can be applied to intranet usage;

WHEREAS, it is in the best interests of the County to offer its elected officials, department heads, and staffs, guidelines and rules for Internet/intranet usage.

The following Internet/intranet Usage Policy is hereby established and becomes part of the Kane County Personnel Handbook and will be distributed to all elected officials and department heads; further, a signed copy of it becomes a permanent part of an employee's personnel file.

Internet/intranet Usage Policy

1. The County provides Internet/intranet access to employees for their use on County business and usage is limited to this function.
2. The County will not monitor individual Internet/intranet usage as a routine matter. There may be a requirement, however, for an elected official, department head, or supervisor to occasionally review individual Internet/intranet usage in their area of responsibility.
3. Staff that access the Internet/intranet must be aware that the hardware and software employed for the Internet/intranet access has the ability to log all County activity, including linked sites.
4. Nothing in this policy shall prohibit law enforcement officials from examining any Internet/intranet usage in the course of an on-going investigation of criminal activity. The County reserves the right to disclose any Internet/intranet activity to law enforcement officials.
5. Any conduct that violates this policy may result in disciplinary action up to and including dismissal.
6. No one shall receive authorized access to the Internet/intranet until he or she has received, reviewed, and agreed to comply with this policy. Such documentation shall be retained in the respective departments.

_____ _____

PRINT NAME DATE

_____

SIGNATURE

18th Judicial Circuit

POLICIES CONCERNING INTERNAL AND EXTERNAL E-MAIL AND USE OF THE INTERNET

The Circuit Judges of the 18th Judicial Circuit have decided to obtain and make available to judges and certain non-judicial personnel of the Circuit certain equipment and technology (computer hardware and software) which will enable users to send and receive internal and external E-Mail and also to access the Internet. The Circuit Judges have decided that certain policies and guidelines should be observed in the use of said technology. A glossary of terms is attached hereto and incorporated herein as a guide to various technical terms.

The equipment and technology provided for both E-Mail and Internet access is provided for business and incidental personal use similar to the purposes presently allowed for telephone and facsimile machines. The primary purposes of this equipment is for the exchange of information in a manner more efficient than available by phone or written memorandum and the gathering of information and research for the court all the while reducing the use of paper to handle information.

Users of this technology are reminded that the same good sense required in our daily lives is necessary for the use of E-Mail and the Internet. It would be a violation of this policy for any user to engage in messages that would be offensive or contain remarks which were insensitive because of their content on a racial, gender, age, disability or other basis. While it is not intended that internal or external E-Mail messages will be monitored, any user should be aware that if an offensive communication somehow becomes public that the sender and perhaps the receiver could be held accountable for the contents of said message. Users of the Internet should be cautioned that it is contrary to the policy of the 18th Judicial Circuit for anyone to access or disseminate any material which is illegal or offensive via chat rooms, web sites or bulletin boards.

Internet users should be cautioned that although passwords may be used that there is no presumption of privacy and that one should presume that communication created, sent, received or stored on the Court's communication system could be read by someone other than the intended recipient.

Each user will maintain two separate E-Mail addresses. One will be public and will be published in various correspondence and directories of the 18th Judicial Circuit. Messages sent to judges at their published addresses will be received by the judge's secretary or other designated non-judicial employee prior to being forwarded to the judge. This will prevent unauthorized communications such as *ex parte* messages from reaching the judge. If the attempted communication is a permissible message, the secretary will forward same to the judge either electronically or by printing a hard copy. If the attempted message is an improper communication, the non-judicial employee will inform the sender that the judge will not accept the message. During periods of a judge's absence the E-Mail sent to the published address will be monitored and handled in the same fashion as paper correspondence.

The private E-Mail address will be known only to the user and may be divulged to other persons at the user's discretion. It is intended that mail sent to the private address will go directly to the user and will be seen by no one else. This, however, does not relieve the sender or receiver of responsibility for an improper or prohibited message that through error or technical malfunction becomes published.

Users of E-Mail are cautioned that any E-Mail correspondence should be given the same consideration as paper correspondence as far as copying, dissemination or retention is concerned. Electronic correspondence may be stored on the user's hard drive. It is advisable for each user to examine their hard drive regularly to purge messages that are no longer necessary.

Users of the Internet are advised that there are many nuances to Internet use and that good judgment should be used at all times. There are certain guidelines that are presumed accepted by anyone who uses equipment or software of the 18th Judicial Circuit for Internet communication:

1. Viruses are always a problem on the Internet. Any user who downloads any material from the Internet must scan same with virus detection software before installing or using the material. Any user who becomes aware of any virus, tampering or any other system security breach should report same to the Court Administrator or his designee immediately.

2. It is never permitted to send, receive or download suggestive, offensive or illegal material on the Internet. Should a violation of this policy be detected the person responsible will be held accountable by the Chief Judge's Office.

3. Users should be mindful that the equipment and software provided is for the purpose of conducting the business of the Circuit and that any personal use of same should be of an incidental nature and be consistent with the public standards of the Circuit.

4. Anyone who uses the Internet to purchase merchandise or services of any type should be cautioned about divulging personal credit card information.

All judicial and non-judicial personnel should understand that the use of the Circuit's computers and software is at the discretion of the Chief Judge. Any violation of these guidelines, policies or procedures as stated above may result in revocation of the privilege of using said equipment or other sanctions as stated in the non-judicial employees policy manual.

The various policies and guidelines for the use of equipment and software of the 18th Judicial Circuit for E-Mail and Internet communication may be modified from time to time.

GLOSSARY

A. ***Electronic Mail (E-Mail):*** Electronic mail may include non-interactive communication of text, data, image or voice messages between a sender and designated recipient(s) by systems utilizing telecommunications links. It may also include correspondence transmitted and stored electronically using software facilities called “mail”, facsimile”, “messaging” systems or voice messages transmitted and stored for later retrieval from a computer system.

B. ***Encryption Software:*** Proprietary software that changes information from its native state to an unrecognizable coded state that can only be returned to its native state with special software.

C. ***Internet:*** A worldwide network of networks, connecting informational networks communicating through a common communications language, or “Protocol.”

D. ***Intranet:*** An in-house web site that serves the users of the 18th Judicial Circuit Court. Although intranet pages may link to the Internet, an intranet is not a site accessed by the general public.

E. ***Judicial Personnel:*** Circuit Judges and Associate Judges of the 18th Judicial Circuit Court.

F. ***List Servers:*** An E-Mail discussion group.

G. ***Worldwide Web:*** An Internet client-server distributed information and retrieval system based upon hypertext transfer protocol (http) that transfers hypertext documents that can contain text, graphics, audio, video and other multimedia file types across a varied array of computer systems.

H. ***Non-Judicial Staff:*** Non-judicial employee’s of the 18th Judicial Circuit Court.

I. ***User:*** Judicial personnel, non-judicial staff, volunteers, contractors and consultants.

NINETEENTH JUDICIAL CIRCUIT, LAKE COUNTY ELECTRONIC POLICY AND PROCEDURES

ELECTRONIC COMMUNICATIONS

1. **Introduction/Purpose**: This policy is intended to serve as a guide on the proper use of the Nineteenth Judicial Circuit Court, Lake County ("NJCC") electronic communication systems. This policy covers the use of all forms of electronic communications including but not limited to e-mail, voice mail, fax machines, external electronic bulletin boards, Intranet, and the Internet, and applies to all Users. Users are expected to read, understand and follow the provisions of this policy and will be held responsible for knowing its contents. Use of the NJCC electronic communication system constitutes acceptance of this policy and its requirements.

   The NJCC provides electronic mail (e-mail) and/or Internet access to Judicial Personnel and Nonjudicial Staff who need it to perform the functions of their position. The purpose of this document is to communicate to all Judicial Personnel and Nonjudicial Staff their responsibility for acceptable use of the Internet and e-mail (whether sent over the Internet or over the NJCC's own network). Policies and procedures are also outlined for the disclosure and monitoring of the contents of e-mail messages stored in the system when required.

   The NJCC's objectives for Judicial Personnel and Nonjudicial Staff to use e-mail and/or the Internet include: 1) exchanging information more efficiently than by telephone or written memorandum; 2) gathering information and performing research for the Court; and 3) reducing the handling of paper copy.

2. **Policy Definitions**: As used in this Policy, the terms listed below shall be defined as follows:

   A. Electronic Mail (e-mail): Electronic mail may include non-interactive communication of text, data, image, or voice messages between a sender and designated recipient(s) by systems utilizing telecommunications links. It may also include correspondence transmitted and stored electronically using software facilities called "mail", "facsimile", "messaging" systems or voice messages transmitted and stored for later retrieval from a computer system.

   B. Encryption Software: Proprietary software that changes information from its native state to an unrecognizable coded state that can only be returned to its native state with special software.

   C. Internet: A worldwide network of networks, connecting informational networks communicating through a common communications language, or "Protocol."

   D. Intranet: An in-house web site that serves the Users of the NJCC. Although intranet pages may link to the Internet, an intranet is not a site accessed by the general public.

   E. Judicial Personnel: Associate Judges and Circuit Judges of the Nineteenth Judicial Circuit, Lake County.

   F. List Servers: An e-mail discussion group.

G. World Wide Web: An Internet client-server distributed information and retrieval system based upon hypertext transfer protocol (http) that transfers hypertext documents that can contain text, graphics, audio, video, and other multimedia file types across a varied array of computer systems.

H. Nonjudicial Staff: Nonjudicial employee's of the Nineteenth Judicial Circuit, Lake County.

I. User: Judicial Personnel, Nonjudicial Staff, volunteers, contractors, and consultants.

3. **Ownership.** The electronic communications system is the property of the NJCC. All computer equipment, computer hardware, and computer software provided by the NJCC are the property of the NJCC. All communications and information transmitted by, received from, or stored in these systems are the property of the NJCC.

4. **Use of Electronic Communications**. NJCC's electronic communication systems, including e-mail and the Internet, are intended for business use only. Incidental and occasional use of these systems for non-work purposes may be permitted at the discretion of the department head or Chief Judge.

   Before using these systems for business or personal use, all Users must understand that any information that is created, sent, received, accessed or stored in these systems will be the property of the NJCC and will not be private. If a User is permitted to use electronic communication systems for non-work purposes, such use shall not violate any section of this policy or interfere with the User's work performance.

   Users should use the same care and discretion when writing e-mail and other electronic communications as they would with any formal written communication. Any messages or information sent by Users to other individuals via electronic communication systems such as the Internet or e-mail are statements identifiable and attributable to the NJCC. Consequently, all electronic communications sent by Users, whether business or personal, must be professional and comply with this policy.

5. **Prohibited Communications.** Under no circumstances may any User operate the NJCC's electronic communication systems for creating, possessing, uploading, downloading, accessing, transmitting or distributing material that is illegal, sexually explicit, discriminatory, defamatory or interferes with the productivity of coworkers. Specifically prohibited communications include, but are not limited to, communications that promote or transact the following: illegal activities; outside business interests; malicious use; personal activities (including chat rooms); jokes; political causes; football pools or other sorts of gambling; recreational games; the creation or distribution of chain letters; list servers for non-work purposes; "spams" (mailing to a large number of people that contain unwanted solicitations or information); sexual or any other form of harassment; discrimination on the basis of race, creed, color, gender, religion, or disability; or for solicitations or advertisements for non-work purposes. Users may not engage in any use that violates copyright or trademark laws. Also prohibited is any activity that could negatively impact public trust and confidence in the NJCC or creates the appearance of impropriety.

Users are also prohibited from posting information, opinions, or comments to Internet discussion groups (for example: news groups, chat, list servers or electronic bulletin boards) without prior authorization from department head or the Chief Judge. Under no circumstances may any User represent their own views as those of the NJCC.

Users may not use e-mail to disclose confidential or sensitive information. Personal information such as the home addresses, phone numbers and social security numbers of Judicial Personnel or Nonjudicial Staff should never be disclosed on the Internet.

6. **No Presumption of Privacy.** Although Users may use passwords to access some electronic communication systems, these communications should not be considered private. Users should always assume that any communications, whether business-related or personal, created, sent, received or stored on the NJCC's electronic communication systems may be read or heard by someone other than the intended recipient.

Users should also recognize that e-mail messages deleted from the system may still be retrieved from the computer's back-up system when requested by authorized personnel. Consequently, messages that were previously deleted may be recreated, printed out, or forwarded to someone else without the User's knowledge.

7. **The NJCC's Right to Monitor Use.** Under authorization of the Chief Judge, the NJCC may monitor, intercept, access, and disclose all information created, sent, received, or stored on its electronic communication systems at any time, with or without notice to the User. The contents of computers, voice mail, e-mail and other electronic communications will be inspected when there are allegations that there have been breaches of confidentiality, security, or violations of this Electronic Communications Policy. These inspections will also be conducted when it is necessary to locate substantive information that is not readily available by less intrusive means.

The contents of the of computers, voice mail, e-mail and other electronic communications may be turned over to the appropriate authority when there are allegations that there have been violations of law.

Before providing access to stored electronic communications such as e-mail messages, written authorization will be required from the Chief Judge. In addition, the NJCC will regularly monitor and maintain a log of the User's Internet access including the type of sites accessed, the name of the server and the time of day that access occurs. The Chief Judge or the Executive Director will have access to this log upon request. The Chief Judge may use information obtained through monitoring as a basis for Nonjudicial Staff discipline.

The Chief Judge may authorize individuals, for investigative purposes, to engage in activities otherwise prohibited by this policy.

8. **Prohibited Activities.** Users may not, without the authorization of the Chief Judge or the Executive Director, upload, download, or otherwise transmit copyrighted, trademarked, or patented material; trade secrets; or confidential, private or proprietary information or materials. Users may not upload, download, or otherwise transmit any illegal information or materials. Users may not use the NJCC's electronic communication systems to gain unauthorized access to remote computers or other systems or to damage, alter, or disrupt such

computers or systems in any way, nor may Users, without authorization from their department head, use someone else's code or password or disclose anyone's code or password including their own. It is a violation of this policy for Users to intentionally intercept, eavesdrop, record, or alter another person's Internet and e-mail messages. Users may not allow unauthorized individuals to have access to or use the NJCC's electronic communication systems, or otherwise permit any use that would jeopardize the security of the NJCC's electronic communication systems. Also, Users may not post an unauthorized home page or similar web site.

Users may not make unauthorized commitments or promises that might be perceived as binding the NJCC. Users must use their real names when sending e-mail messages or other electronic communications and may not misrepresent, obscure or in any way attempt to subvert the information necessary to identify the actual person responsible for the electronic communication. Sending an e-mail message under a fictitious or false name is a violation of this policy. Likewise, using another Users account or login ID constitutes a violation of this policy.

9. **Passwords**. Each User will maintain a unique password. Users must keep their passwords confidential and must never leave their computers unattended when logged onto the system. Passwords shall be changed whenever a password may have been compromised or revealed or when the computer security system requests a new password.

Directories of User e-mail addresses may not be made available for public access. No visitors, contractors or temporary employees may use NJCC e-mail without prior written authorization from the Chief Judge or the Executive Director.

10. **Internet Usage.** Access to the Internet from any PC connected to the NJCC network is only allowed in accordance with this policy. Alternate methods of Internet access, such as using a modem to access America On-Line, may compromise the NJCC's network security exposing it to potential harm from computer hackers. Requests for exceptions to this rule must be reviewed and approved by the Chief Judge or Executive Director in consultation with the Judicial Information Systems Manager.

Sessions on the Internet are logged automatically in exactly the same way that phone numbers are logged in the phone systems. Do not use the Internet for tasks that you would not want logged.

Web browsers leave "footprints" providing a trail of all site visits. Do not visit any site where you would be reluctant to leave your name and work location. Use appropriate judgment before filling out a form included in a Web page. The form will pass through many interconnecting computers and networks before reaching its destination. Other individuals will be able to eavesdrop on it. Personal or valuable information on the form may not remain confidential. Under no circumstances should you ever put a Social Security number on the Internet.

An Internet message sent from the Court's address constitutes a Court communication. Therefore, it should be composed and structured correctly. Whenever possible, spell-check messages prior to transmission, especially when sending to a non-Court address.

Sending e-mail from the Court's address can be likened to sending a letter on Court letterhead. Messages may be forwarded to others by the recipient, printed in a location where others may view the message, and/or directed to the wrong recipient. Also, computer forensic experts can often retrieve e-mail previously deleted. An ill-considered remark can return to haunt the sender later.

Be courteous and follow generally accepted standards of etiquette. Protect others' privacy and confidentiality. Consider Court needs before sending, filing, or destroying e-mail messages. Remove personal messages, temporary records, and duplicate copies in a timely manner.

11. Records Retained. Certain significant types of e-mail messages or their attached files may be considered records and should be retained if required by the Court's record-retention policies**.** Examples of messages sent by e-mail that may constitute records include: 1) policies and directives; 2) correspondence or memoranda related to official business; 3) work schedules and assignments; 4) agendas and minutes of meetings; 5) drafts of documents that are circulated for comment or approval; 6) any document that initiates, authorizes, or completes a business transaction; and 7) final reports or recommendations.

12. Records Disposal. The content and maintenance of a User's electronic mailbox are the User's responsibility. The content and maintenance of a User's disk storage area are the User's responsibility. Each User should review his/her electronic records for deletion every thirty (30) days. Messages of transitory or little value that are not normally retained in record-keeping systems should be regularly deleted. Informational messages such as meeting notices, reminders, informal notes, and telephone messages should be deleted once the administrative purpose is served. If it is necessary to retain any e-mail message for an extended period, transfer it from the e-mail system to an appropriate electronic or other filing system. With the approval of the Chief Judge, the Judicial Information System Manager is permitted to remove any information retained in an e-mail system more than thirty (30) days old.

13. Accessing User E-mail During Absence. During a User's absence, the Chief Judge or Executive Director may authorize the Judicial Information Systems Manager to access the User's E-mail messages and electronic Internet records without the consent of the User when necessary to carry out normal business functions.

The Executive Director shall notify the User in writing when information under the User's control has been accessed. Such notification shall be made within 48 hours of the access or within 48 hours of the User's return to work.

14. Licensing Fees. Users may not install any software for which the NJCC has not paid the appropriate licensing fee. Additional licensing fees may be incurred every time software is installed for a new User. Consequently, before software is installed on their computer, Users have a duty to ensure that all appropriate licensing fees have been paid. Users should notify their Division Director or Judicial Information Systems if they discover unlicensed software on their computer.

Users may not copy software for distribution to any third party or for home use unless such copying is permitted by the software's license agreement. The installation of software for trial periods authorized by the vendor would not be a violation of this policy. Such software must be approved and installed by Judicial Information Systems.

15. **Password Protection.** Users should not encryption software or otherwise password protect their files. Frequently, password protected files cannot be retrieved without the necessary password. The NJCC is not responsible for any lost, damaged, or inaccessible files that results from password protection.

16. **Viruses and Tampering.** Any files downloaded from the Internet must be scanned with virus detection software before installation and execution. The intentional introduction of viruses, attempts to breach system security, or other malicious tampering with any of the NJCC's electronic communication systems is expressly prohibited. Users must immediately report any viruses, tampering, or other system breaches to the Judicial Information Systems Manager.

17. **Disclaimer of Liability for Use of the Internet.** The NJCC is not responsible for material viewed or downloaded by users from the Internet. The Internet provides access to a significant amount of information, some of which contains offensive, sexually explicit and inappropriate material. It is difficult to avoid contact with this material, therefore users of the Internet do so at their own risk.

18. **Duty Not to Waste Electronic Communications Resources.** Users must not deliberately perform actions that waste electronic communication resources or unfairly monopolize resources to the exclusion of other Users. This includes, but is not limited to, subscribing to list servers, mailing lists or web sites not directly related to the User's job responsibilities; spending extensive nonproductive time on the Internet; and doing large non-work related file downloads, or mass mailings. Electronic communication resources are limited and Users have a duty to conserve these resources.

19. **Non-Work Related Global E-mail.** A non-work related global e-mail message is one sent to multiple users outside the NJCC's system that is unrelated to the Users work duties. Prior approval of either the Executive Director or the Judicial Information Systems Manager is required to send a non-work related global E-mail.

20. **E-mail Addresses.** The NJCC reserves the right to keep a User's e-mail address active for a reasonable period of time following the User's departure to ensure that important business communications reach the Court.

21. **Freedom of Information Act Requests.** The NJCC will not accept Freedom of Information Act (F.O.I.A.) requests from the public via the Internet. If a citizen e-mails a F.O.I.A. request to a User, the employee should notify the citizen that these requests must be made in writing and addressed to the attention of the Chief Judge or the Executive Director.

22. **Use of Credit Cards on the Internet.** Before making purchases on the Internet, Users who are authorized to use NJCC credit cards must ensure that they are using a secured site. The NJCC recommends that Users do not use their credit cards over the Internet and expressly disclaims responsibility for any loss or damage that results from credit card usage over the Internet.

23. **Violations – Nonjudicial Staff.** Violations of this policy may subject Nonjudicial Staff to disciplinary action ranging from the removal of electronic communication privileges to dismissal from employment. Nonjudicial Staff who observe violations of this policy are

obligated to report the violations to the Chief Judge, Executive Director, or Judicial Information Systems Manager.

24. Violations – Judicial Personnel. Violations of this policy will be reviewed and acted upon solely by the Chief Judge.

25. Policy Changes. The NJCC reserves the right to change this policy at any time without notice. Nothing in this policy is intended or should be construed as an agreement and/or a contract, express or implied. Policy changes will be disseminated electronically or in written form within forty-eight (48) hours of taking effect.